**БЕКІТІЛДІ**

«Әлеуметтік медициналық сақтандыру қоры» КЕАҚ Директорлар кеңесінің 2023 жылғы «1» маусымдағы шешімімен (№ 10 хаттама)

«Әлеуметтік медициналық сақтандыру қоры» КЕАҚ

ақпараттық қауіпсіздік саясаты

Астана, 2023 жыл

**Мазмұны**

|  |  |
| --- | --- |
| 1. Жалпы ережелер | 3 |
| 2. Ақпараттық қауіпсіздік саясатының мақсаты мен міндеттері | 4 |
| 3. Ақпараттық қауіпсіздікті қамтамасыз етудің жетекші принциптері | 6 |
| 4. Ақпараттық қауіпсіздікті қамтамасыз етудің практикалық әдістері | 6 |
| 5. Қорытынды ережелер | 7 |

**1. Жалпы ережелер**

1. «Әлеуметтік медициналық сақтандыру қоры» КЕАҚ ақпараттық қауіпсіздік саясаты (бұдан әрі - АҚС) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мақсаттарды, міндеттерді, басшылық қағидаттар мен практикалық тәсілдерді (бұдан әрі – АҚ) айқындайтын бірінші деңгейдегі құжат болып табылады.
2. АҚС төмендегілерге сәйкес әзірленген:

1) «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы;

2) Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптармен (бұдан әрі-Бірыңғай талаптар);

3) ISO/IEC 27000, COBIT, ITIL ақпараттық қауіпсіздігі бойынша халықаралық стандарттар сериясы, Қордың ақпараттық инфрақұрылымын дамытудың қазіргі жағдайы мен таяудағы перспективалары, сондай-ақ ақпаратты қорғаудың заманауи ұйымдастырушылық-техникалық әдістерінің мүмкіндіктері;

1. АҚС ережелерін «Әлеуметтік медициналық сақтандыру қоры» КЕАҚ-тың (бұдан әрі-Қор) барлық қызметкерлері, тағылымдамадан өтушілер, практиканттар орындауға міндетті, сондай-ақ Қордың ақпараттық жүйелері мен құжаттарына қолжетімділігі бар өзге де үшінші тұлғалардың назарына Қормен және олардың қызметімен тікелей өзара байланысты бөлігінде жеткізілуі тиіс.
2. АҚС иесі және пайдаланушысы Қор болып табылатын барлық ақпараттық жүйелер мен құжаттарды қамтиды.

Ақпараттық қауіпсіздікті қамтамасыз ету – Қор қызметін табысты жүзеге асыру, дербес ақпаратты қорғау, сондай-ақ заңнамаға сәйкестікті қамтамасыз ету үшін қажетті шарт болып табылады. Ақпарат Қордың маңызды активтерінің бірі болып табылады. Ақпараттық қауіпсіздіктің жоғары деңгейін ұстап тұру Қордың оның қауіпсіздігін қамтамасыз ету саласындағы бірыңғай саясатының маңызды бағыты болып табылады.

1. Қордың АҚ – бұл оның ақпараттық активтерінің материалдық зиян келтіруге, Қордың беделіне нұқсан келтіруге немесе Қорға, жұмысшыларға немесе клиенттерге өзге де залал келтіруге әкеп соғуы мүмкін кездейсоқ немесе қасақана әсерлерге орнықтылығының (қорғалуының) жай-күйі.
2. Қор ұсынатын АҚ талаптары «Әлеуметтік медициналық сақтандыру қоры» КЕАҚ – ның 2020-2025 жылдарға арналған даму стратегиясына сәйкес келеді және АҚ-мен байланысты тәуекелдерді қолайлы деңгейге дейін төмендетуге арналған. Қордың АҚ саласында тәуекелдердің болуы оның корпоративтік басқаруына (менеджментіне), бизнес-процестерді ұйымдастыруға және іске асыруға, контрагенттермен және клиенттермен өзара қарым-қатынастарға, шаруашылықішілік қызметке қатысы бар. Қордың АҚ саласында тәуекелдердің болуы Қордың операциялық тәуекелдерінің бір бөлігін құрайды, сол арқылы Қордың негізгі қызметіне әсер етеді.
3. Қор басшылығы Қордың тиімді және тұрақты жұмысын қамтамасыз етуге, сондай-ақ барлық мүдделі тараптардың Қор жұмысының сенімділігі мен тұрақтылығына, олардың мүдделерінің әртүрлі қолайсыз факторлардың әсерінен қорғалуына сенімділігін қолдауға ұмтылады.
4. Басшылық ақ Қордың табысты және тұрақты жұмысының маңызды факторларының бірі болып табылатынын және АҚ қамтамасыз етудің мақсаттары мен қағидаттарына қажетті жәрдем көрсетуге және міндеттеме көрсетуге ниетті екенін түсінеді. Қор басшылығы АҚ басқару процесін жалпы бақылауды өзіне қалдырады.

8-1. Басшылық Қор қызметкерінің және орындаушылар тарапынан тартылатын ақпараттық қауіпсіздік міндеттемелері мен талаптарын орындау мүмкіндігін қамтамасыз етеді.

8-2. Басшылық ақпаратты қауіптер мен тәуекелдерден қорғауды қамтамасыз ететін ішкі құжаттар мен рәсімдерді әзірлеуге қатысады.

8-3. Басшылық қаржылық, материалдық және адами ресурстарды қоса алғанда, ақпараттың қауіпсіздігін қамтамасыз ету үшін жеткілікті ресурстарды қамтамасыз етеді.

**2. АҚС мақсаты мен міндеттері**

1. АҚС құру мен жетілдірудің негізгі мақсаттары:

1) Қор үшін оның маңыздылығына қарай ақпараттың тиісті қорғалуын қамтамасыз ету;

2) ақпараттың құпиялылығын, түпнұсқалығын, тұтастығын қамтамасыз ету, дербес деректерді қорғау;

3) Қордың ақпаратына және ақпаратты өңдеу құралдарына рұқсатсыз физикалық қол жеткізуді, зақымдануды және араласуды болдырмау;

4) ақпараттық жүйелердің ажырамас бөлігі ретінде ақпараттық қауіпсіздікті олардың бүкіл өмірлік циклі ішінде қамтамасыз ету;

5) қауіпсіздік оқиғалары туралы хабарламалар мен әлсіз жақтарын қоса алғанда, ақпараттық қауіпсіздік инциденттерін басқарудың үздіксіз және нәтижелі тәсілін қамтамасыз ету.

1. АҚС-ны табысты іске асыру мақсатында мынадай міндеттерді нәтижелі орындау қажет:

1) Қордың ақпараттық активтерін түгендеу және жіктеу;

2) АҚ тәуекелдерін және осы тәуекелдердің әлеуетті мүмкіндіктерін анықтау;

3) АҚ қамтамасыз етудің негізгі талаптары мен рәсімдерін айқындау және құжаттау;

4) ақпаратты қорғау құралдарын енгізу және баптау;

5) Қор қызметкерлерін АҚ саласында оқыту;

6) Қор активтерінің осалдығын уақтылы анықтау және жою және сол арқылы Ақ қатерлерін іске асыру нәтижесінде Қордың бизнес-процестерінің қалыпты жұмыс істеуіне нұқсан келтіру және бұзылу мүмкіндігінің алдын алу;

7) АҚ қатерлерін іске асыру кезінде Қордың ықтимал залалын қолайлы деңгейге дейін азайту, оның ішінде ықтимал үзілістерден кейін бизнес-процестерді қалпына келтіру уақытын қысқарту;

8) АҚ оқиғалары мен инциденттерін мониторингілеу және өңдеу;

9) Қордың ақпараттық қауіпсіздігін қамтамасыз етуге арналған шығындарды жоспарлау және оңтайландыру.

1. Ақпараттық технологиялар (бұдан әрі - АТ) саласындағы Қордың тәуекелдерін бағалау негізінде АҚ-ны қамтамасыз ету жөніндегі ұйымдастырушылық және техникалық шаралар кешенін жоспарлау, іске асыру және бақылау:
2. Қордың бизнес-процестерін қолдау үшін оның ақпараттық активтерінің үздіксіз қолжетімділігін қамтамасыз ету;
3. бизнес-процестердің жоғары сапасын қолдау мақсатында Қордың ақпараттық активтерінің тұтастығын қамтамасыз ету;
4. ақпараттың түпнұсқалығын, тұтастығын құпиялылықты қамтамасыз ету, дербес деректерді қорғау;
5. Қорда қолданылатын ақпараттық қауіпсіздік бойынша қабылданатын шаралардың заңнама талаптарына, сондай-ақ реттеуші және қадағалау ұйымдарының талаптарына сәйкестігін қамтамасыз ету.
6. Қорғалатын объектілер:
7. Қордың жұмыс істеуі үшін қажетті ақпараттық активтер, оларды ұсыну нысаны мен түріне қарамастан;
8. ақпараттық технологияларды, ақпаратты қалыптастыру, өңдеу, беру, сақтау (оның ішінде архивтелген) және пайдаланудың техникалық және бағдарламалық құралдарын қоса алғанда, ақпараттық жүйелер,
9. компьютерлік техниканы, кітапханаларды, мұрағаттарды, деректер базасын, серверді қоса алғанда, АТ-инфрақұрылымының элементтері, орталық аппарат пен филиалдардағы физикалық және виртуалды арналарды, ақпарат алмасу және телекоммуникация арналарын, ақпаратты қорғау жүйелері мен құралдарын, Қордың АТ-инфрақұрылымының қорғалатын элементтері орналасқан объектілер мен үй-жайларды қоса алғанда;
10. Орталық аппарат пен филиалдарды қоса алғанда, Қордың құрылымдық бөлімшелері,
11. Қордағы ақпаратты өңдеу процестері, регламенттері мен рәсімдері;
12. қызметкерлердің дербес деректері және Қор жеткізушілерінің деректемелері.
13. Қорға меншік құқығында (оның ішінде зияткерлік меншік құқығында) Қазақстан Республикасының қолданыстағы заңнамасына сәйкес қызметті жүзеге асыру мақсатында сатып алынған (алынған) және пайдалануға берілген барлық іскерлік ақпарат пен есептеу ресурстары тиесілі. Аталған меншік құқығы Қордың жабдықтарын пайдалана отырып жүзеге асырылатын дауыстық, лицензиялық және әзірленген бағдарламалық қамтамасыз етуге, электрондық пошта жәшіктерінің мазмұнына, Қордың барлық функционалдық бөлімшелері мен қызметкерлерінің қағаз және электрондық құжаттарына қолданылады.

**3. Ақпараттық қауіпсіздікті қамтамасыз етудің жетекші принциптері**

1. АҚС мына принциптерге негізделген:
2. ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтау арқылы АҚ қамтамасыз ету;

2) ақпаратқа тек уәкілетті тұлғаларға рұқсат беру арқылы құпиялылық;

1. жалпыға қолжетімді электрондық ақпараттық ресурстарға (дербес компьютерлердегі, корпоративтік электрондық поштадағы, ЭҚЖ және т. б. деректерге) тек қана рұқсат етілген өзгерістер енгізу жолымен тұтастығы;
2. уәкілетті тұлғаларға қызметтік міндеттерін орындау үшін жалпыға қолжетімді электрондық ақпараттық ресурстарға қолжетімділік беру (дербес компьютерлердегі, корпоративтік электрондық поштадағы, ЭҚЖ және т. б. деректер).

**4. Ақпараттық қауіпсіздікті қамтамасыз етудің практикалық әдістері**

1. Қордың АҚ мәселелеріне жалпы басшылықты Қор басшылығы жүзеге асырады, оның АҚ контекстіндегі міндеттеріне мыналар кіреді:
2. Қазақстан Республикасының ақпараттық-коммуникациялық технологиялар және олардың ақпараттық қауіпсіздігі саласындағы заңнамасына сәйкес АҚ мақсаттарын тиісті процестерде қамтамасыз ету;
3. АҚС бекіту;
4. Қорда АҚ басқару жөніндегі іс-шараларды енгізуді үйлестіруді жүзеге асыру;
5. АҚ саласындағы бастамаларды нақты басқаруды және нақты қолдауды қамтамасыз ету;
6. АҚ қамтамасыз ету үшін қажетті ресурстарды бөлу;
7. АҚ-ға қатысты негізгі міндеттер мен функцияларды бөлуді бекіту;
8. АҚ қамтамасыз ету саласындағы жауапкершілік пен функциялардың аражігін ажырату мақсатында ақпараттандыру объектілерін құру, сүйемелдеу және дамыту мәселелерімен айналысатын құрылымдық бөлімше болып табылатын Өзіндік қауіпсіздік департаментінің Ақпараттық қауіпсіздік басқармасы құрылады немесе АҚ-ны қамтамасыз етуге жауапты лауазымды адам айқындалады.:
9. АҚ бойынша техникалық құжаттама талаптарының орындалуын бақылау;
10. АҚ-ның құжаттамалық ресімделуін бақылау;
11. АҚ-ны қамтамасыз ету бөлігінде активтерді басқаруды бақылау;
12. бағдарламалық қамтамасыз етуді пайдаланудың заңдылығын бақылау;
13. АҚ саласындағы тәуекелдерді басқаруды бақылау;
14. АҚ оқиғаларының тіркелуін бақылау;
15. АҚ ішкі аудитін жүргізу;
16. АҚ сыртқы аудитін ұйымдастыруды бақылау;
17. ақпараттық-коммуникациялық технологияларды пайдаланатын бизнес-процестердің үздіксіздігін қамтамасыз етуді бақылау;
18. персоналды басқару кезінде ақ талаптарының сақталуын бақылау.

**5. Қорытынды ережелер**

1. Қордың, оның филиалдарының басшылығы АҚ-ны қамтамасыз ету жөніндегі қызмет үшін жауапты болады, жоғарыда көрсетілген мақсаттар мен қағидаттарға өзінің адалдығын мәлімдейді.
2. Қордың, оның филиалдарының қызметкерлері АҚС талаптарының сақталуына жауапты болады және АҚ саласында анықталған барлық бұзушылықтар туралы уақтылы хабарлауға тиіс.
3. Осы Саясаттың ережелерін қайта қарау тұрақты негізде, бірақ кемінде екі жылда бір рет жүзеге асырылады.
4. Осы Саясатты жоспардан тыс қайта қарау мынадай жағдайларда жүзеге асырылады:

1) Қазақстан Республикасының нормативтік құқықтық актілеріне, ақпараттық қауіпсіздік талаптарын айқындайтын Қордың ішкі құжаттарына өзгерістер енгізу;

2) Қордың ақпараттық қауіпсіздігінің жалпы деңгейінің төмендеуін анықтау (ішкі немесе сыртқы аудит нәтижелері бойынша);

3) Қордың ұйымдық және / немесе инфрақұрылымына, ресурстарына және бизнес-процестеріне елеулі өзгерістер енгізу;

4) осы Саясатпен регламенттелген іс-шараларды орындау кезінде елеулі кемшіліктерді, сондай-ақ оның ережелерінің Қордың басқа ішкі құжаттарымен қайшылықтарын анықтау.

1. Осы Саясатты қайта қарау, сондай-ақ оған өзгерістер енгізу Қордың ішкі құжаттарында белгіленген тәртіпке сәйкес орындалады.